UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,525	01/25/2001	Michael Hrabik	881075/3	5856

7590 06/02/2005

Joel E. Lutzker, Esq.
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/770,525	HRABIK ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 23-41 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 23-30,32-35 and 39-41 is/are rejected.

7)☒ Claim(s) 31, 36-38 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 24-27, 34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims 24, 34, recites wherein the first communication medium is connected only to the security subsystem and to the master system, and not to any of the network devices. Claim 24, is not described in the specification. In the specification on page 5, the subsystem is connected via a secure link to a master system that is not otherwise connected to the target system. Claim 24 is not disclosed in the specification. Further, a first communication medium is not disclosed anywhere in the specification. Claim 25, is not enabled, what is disclosed is, if the subsystem detects an attack on the target network, or does not respond to the master system, the master system will take appropriate action, ranging from logging the incident or notifying a network manager to shut down the network(see pg. 5 of spec). The attack in the disclosure refers to the subsystem; Claim 25 is not disclosed in the specification. As per claim 26, there is disclosed a second communication medium. In the specification, on page 7, what is disclosed is a secure link that may be established through an encrypted communication protocol. Claim 26, is rejected under 112 1st. Claim 27 is rejected under 112 1st because it is dependent on claim 26.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 23, 28-29, 33, 40-41 are rejected under 35 U.S.C. 102(b) as being anticipated by Emigh.

5. As per claims 23, 33, Emigh teaches a security system(i.e. netranger sensor) for a computer network, the network having a plurality of devices connected thereto (see lines 1-4, 28-30), a security subsystem connected to at least some of the devices in the network(see lines 28-30), the security subsystem configured to monitor activities of the at least some devices on the network(see lines 28-32), and detect attacks on the at least some devices(see lines 33-36); a master system(i.e. IBM's Network Security Operations Center(NSOC) which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem(see lines 1-6, 37-43); and a first communication medium; inherent in Emigh, because Emigh teaches that if a misuse is found it can be sent in real-time to the NSOC in Boulder, Colorado(see lines 33-36), connected between the security subsystem and the master system(see lines 33-36), the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks thorough the first communication medium(see lines 1-6, 37-43).

6. As per claim 28, Emigh teaches the master system is hierarchically independent from the security subsystem(see lines 1-6).

7. As per claim 29, Emigh teaches that the security subsystem is hierarchically subordinate to the master system(see lines 28-32).

8. As per claims 40, Emigh inherently teaches at lest one of the devices having a security related functions is a firewall, because Emigh teaches that the sensor can be located on places of the internet or intranet connections (see lines 28-32).

9. As per claim 41, Emigh teaches wherein at least one of the devices having security related functions is a network intrusion detection system(see lines 1-6).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 30, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of Messmer.

12. As per claims 30, 39, Emigh is silent on wherein the first communication medium is a secure link defined by a virtual private network tunnel; however, Messmer teaches the link it output in encrypted form(i.e. vpn). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a secure link by a virtual private network tunnel of Messmer with Emigh, the motivation is that network activity is output in encrypted form and prevents hackers or intruders from viewing information(see Messmer).

13. Claims 30, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of Kurtzberg.

14. As per claim 32, 35, Emigh teaches a master system(see lines 5-6), security subsystem(see lines 1-4), detecting attacks(see lines 33-36). Emigh does not teach a pseudo-attack generator, which generates attacks on the network, and determining whether the integrity of the system has been compromised. Kurtzberg et al. discloses a pseudo-attack generator which generates attacks on the network, and determining whether the integrity of the system has been compromised(see col. 1, lines 40-67). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a pseudo-attack generator which generates attacks on the network, and determining whether the integrity of the system has been compromised of Kurtzberg with Emigh, the motivation if that the integrity of a computer system can be tested reliably to improve or complement the system's performance(see col. 1, lines 65-67 of Kurtzberg).

15. Claims 31, 36, 37-38 are objected to as being rejected on base claims. The reasons why the claims are allowable are because in the prior art of security, networking and non-patent literature, prior art fails to disclose or suggest, when the master system monitors whether the security subsystem responds to the master system, the master system taking action. The master system monitors the security subsystem in prior art and all data for network devices is transmitted to the master system, there is no suggestion or disclosure of this limitation.

Response to Amendment

16. The Applicant's arguments were persuasive and therefore, the new art has been applied, and thus remarks by Applicant are moot.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

May 29, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100